

NDB/RMP  
F. #2023R00222/NY-NYE-865

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF (1)  
AN IPHONE 14 WITH IMEI NUMBER  
89382000180005018276, (2) A GREY  
SAMSUNG PHONE WITH IMEI  
350867/77/455671/4, AND (3) A BLACK  
SAMSUNG PHONE WITH IMEI NUMBER  
350699/18/670253/1, ALL IN  
GOVERNMENT CUSTODY IN THE  
EASTERN DISTRICT OF NEW YORK

**APPLICATION FOR A  
SEARCH WARRANT FOR  
ELECTRONIC DEVICES**

Case No. 24 MC 3226

**AFFIDAVIT IN SUPPORT OF AN  
APPLICATION UNDER RULE 41 FOR A  
WARRANT TO SEARCH AND SEIZE**

I, William H. Jambois, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—three electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a special agent with the Department of Homeland Security, Homeland Security Investigations (“HSI”), which I have been since earlier this year. Prior to becoming an HSI special agent, I worked for U.S. Customs and Border Protection for approximately ten years, first as a border patrol agent and then as a supervisor. In my current role, my official duties include conducting and assisting in investigations into the activities of

individuals and criminal groups responsible for, among other things, engaging in the illegal trafficking, distribution, and possession of narcotics. Over the course of my career, I have participated in investigations and arrests, the debriefing of cooperating witnesses and confidential informants, and the execution of warrants related to various types of criminal activity, including drug-trafficking. I have experience with a variety of investigative techniques, including but not limited to (i) executing search warrants; (ii) reviewing and analyzing communications among members of criminal groups, including electronic messages; (iii) obtaining and analyzing location information for cellular telephones; (iv) conducting physical surveillance; (v) reviewing surveillance footage; and (vi) interviewing suspects and witnesses.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

**IDENTIFICATION OF THE DEVICE TO BE EXAMINED**

4. The property to be searched is (1) an iPhone 14 with international mobile equipment identity (“IMEI”) number 89382000180005018276, (2) a grey Samsung phone with IMEI number 350867/77/455671/4, and (3) a black Samsung phone with IMEI number 350699/18/670253/1, hereinafter the “Devices.” The Devices are currently in government custody in the Eastern District of New York.

5. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

**PROBABLE CAUSE**

6. On September 15, 2023, a grand jury sitting in the Eastern District of New York returned a superseding indictment charging Milos Radonjic with international conspiracy and attempt to violate the Maritime Drug Law Enforcement Act (“MDLEA”), in violation of 46 U.S.C. §§ 70503(a)(1), 70503(b), 70504(b)(2), 70506(a), 70506(b), and 70507(a), 18 U.S.C. § 2, and 21 U.S.C. § 960(b)(1)(B)(ii). See United States v. Milos Radonjic, et al., 23-CR-257 (S-1) (ARR). On October 6, 2023, Radonjic was arrested by Italian authorities at the United States government’s request when Radonjic entered Italy for a yacht race in which he was expected to compete as the captain of a racing yacht. On July 26, 2024, Italy extradited Radonjic to the United States. On July 29, 2024, he made his initial appearance and was arraigned on the superseding indictment in the Eastern District of New York, where he was ordered detained pending trial.

7. The charges against Radonjic arose from an extensive federal investigation into the criminal activities of a vast international drug trafficking organization in which Radonjic and his co-conspirators used commercial container maritime vessels that transited from South America to the United States and Europe to transport massive quantities of cocaine for cartels located in the Balkans.

8. Radonjic and his co-conspirators used a variety of messaging applications, including Sky ECC, Signal, iMessage, and Facetime to communicate and coordinate the process of loading the cocaine onto the vessels. Sky ECC was a subscription-based end-to-end encrypted messaging application, formerly operated by Sky Global. Sky Global sold specially modified cellphones (“Sky Phones”), which operated on the Sky ECC network and were intended to be

more secure than typical cell phones. International criminal organizations made extensive use of Sky Phones and the Sky ECC network until a multinational law enforcement operation in early 2021 dismantled the Sky ECC infrastructure, seized its servers, and began decrypting a large cache of communications that remained on those servers.

9. The government has obtained from European law enforcement voluminous records of Radonjic's communications on one Sky Phone (or one Sky ECC account). The government's review of those communications is ongoing. To date, the government has identified within those communications, inter alia, explicit planning and discussion of narcotics trafficking, photographs of parts of one ship that was used to transport narcotics, the geolocation data for that ship, and references to the specific attempts to load cocaine aboard the ship.

10. In addition to Radonjic's overtly criminal communications on the Sky Phone, the Sky ECC data also includes attribution evidence that ties those communications to Radonjic. For instance, Radonjic's (formally anonymous) communications on his Sky Phone include an image of a receipt with Radonjic's true name, address, and phone number; references to international travel that correspond to border crossings and travel reservations in Radonjic's true name; a reference to what appears to be a birthday on Radonjic's daughter's true birthdate; and photographs of a vehicle (with visible license plate) that was registered to a sailor who is a member of Radonjic's yacht racing team.

11. At the time of Radonjic's arrest in Italy, he was in possession of the Devices. Radonjic gave Italian law enforcement authorities consent to search and the passcode to access his iPhone—i.e., one of the Devices for which the government seeks the instant warrant. He claimed that he had forgotten the passcodes to the two Samsung phones that he

carried with him—i.e., the other two Devices for which the government seeks the instant warrant.

12. Pursuant to the government's formal request via treaty to Italy for forensic copies of any extraction reports generated from the Devices, Italian law enforcement provided the government with an extraction report that it generated from Radonjic's iPhone. Italian authorities did not access Radonjic's two Samsung phones.

13. In my training and experience, it is common for international narcotics traffickers to carry multiple cell phones in an attempt to segregate criminal communications from personal ones, and/or to use different phones (and thus different phone numbers) to communicate with different co-conspirators or co-conspirators in distinct roles. Despite that attempted division of criminal and personal communications and/or different categories of criminal communications, users often cross-contaminate their various cell phones with both personal and criminal details like the ones described above.

14. In my training and experience, it is also common for international narcotics traffickers to claim to have forgotten the passcodes to their incriminating cell phones, even if they consent to searches of their personal phones. Indeed, it would be highly unusual to travel with multiple personal cellphones and only know the password for one of them. Accordingly, I assess that it is likely Radonjic falsely denied knowledge of the passwords to his Samsung phones because those phones were used for criminal communications, like those described above that he previously made with his Sky ECC phone before the law enforcement takedown of the Sky ECC network.

15. In my training and experience, people who carry personal cellphones typically carry them all or nearly all the time and use them in ways that generate abundant attribution evidence of the type described above with reference to the attribution evidence from Radonjic's Sky Phones. Indeed, it is very likely that Radonjic used the Devices in some of the same ways that he used his Sky Phone, and that the Devices therefore contain, e.g., evidence of travel, and photographs of distinctive objects, locations, and individuals (including Radonjic's child). Any information on the Devices that matches the attribution evidence on Radonjic's Sky Phone—e.g., geolocation data stored on the Devices that matches travel reflected on the Sky Phones, usernames or passwords that overlap those used or recorded in the Sky Phones, or photographs or other information that show the same individuals, locations, or objects that are depicted in the Sky Phone—is therefore attribution evidence that further ties Radonjic to the Sky Phone and thus to the charged crimes.

16. The Devices are the three cell phones Radonjic was carrying at the time of his arrest, and they were seized incident to arrest. They have been in the continuous lawful possession of Italian and U.S. law enforcement since that time and are currently in HSI's custody within the Eastern District of New York. The Devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into HSI's possession.

17. Accordingly, I submit that there is probable cause to believe that a search of the Devices will reveal evidence of crime, including attribution evidence that corresponds to evidence from the Sky ECC data.

### **TECHNICAL TERMS**

18. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by

connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special



sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.
- f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed

properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

19. Based on my training, experience, and research, I know that the Devices have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

#### **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

20. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

21. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how

the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- h. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- i. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- j. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- k. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

1. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

22. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

23. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

---

CONCLUSION

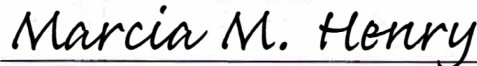
24. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



William H. Jambois  
Special Agent  
Department of Homeland Security, Homeland  
Security Investigations

Subscribed and telephonically sworn to before me  
by telephone on August 16, 2024:



HONORABLE MARCIA M. HENRY  
UNITED STATES MAGISTRATE JUDGE  
EASTERN DISTRICT OF NEW YORK